Claims

1. An information processing system for distributing encrypted message data capable of being used only in not less than one device selected,

said individual device comprising:

encryption processing means for holding a different key set of a node key peculiar to each node in a hierarchical tree structure with a plurality of different devices as leaves and a leaf key peculiar to each device and executing decrypting process on said encrypted message data distributed to a device using said key set;

wherein a message data distributing means generates a renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected at subordinate of a top node which is one node of the hierarchical tree structure is renewed and an enabling key block (EKB) into which said renewal node key is encrypted with a node key or a leaf key in said group, and generating and distributing a message data encrypted with said renewal node key.

2. The information processing system according to claim 1 wherein said encryption processing means in said device obtains said renewal node key by the processing of said enabling key block (EKB) and executing decrypting of said encrypted message data by the renewal node key obtained.

3. The information processing system according to claim 1 wherein said message data is a content key that can be used as a decryption key for decrypting content data.

4. The information processing system according to claim 1 wherein said message data is an authentication key used in the authentication processing.

5. The information processing system according to claim 1 wherein said message data is a key for generateing an integrity check value (ICV) of the content.

6. The information processing system according to claim 1 wherein said message data is a program code.

7. The information processing system according to claim 1 wherein said message data distributing means distributes said enabling key block (EKB) and an encrypted data comprising a content key usable as a decryption key for decrypting content data as said message data and an encrypted content encrypted by said content key.

8. The information processing system according to claim 1 wherein said message data distributing means and said device respectively have an authentication processing means for executing authentication processing, and

wherein a distribution of said message data is performed on the condition that authentication processing between said message data distributing means and said device has been completed.

9. The information processing system according to claim 1 wherein there exists a different intermediate device between said message data distributing means and said device, and

wherein said message data distributing means generates and distributing an

enabling key block (EKB) and an encrypted message data that can be decrypted only in target devices targeted for distributing said message data.

10. The information processing system according to claim 1 wherein said hierarchy tree structure includes a category group constituted as a group, with one node as a top node, containing nodes and leaves connected at subordinate of said top node;

wherein said category group is constructed as a set of devices that belong to a category defined solely by a kind of a device, a kind of a service or a kind of a managing means..

11. The information processing system according to claim 10 wherein said category group further includes one or more sub-category groups in the lower stage of said hierarchy tree structure;

wherein said sub-category group is constructed as a set of groups that belong to a category defined solely by a kind of a device, a kind of a service, a kind of a managing means.

12. An information processing method for distributing from a message data distributing means encrypted message data capable of being used only in not less than one device selected, comprising:

a message data distributing step of generating a renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected at subordinate of a top node which is one node of the hierarchical tree structure

having a plurality of different devices as leaves is renewed, and an enabling key block (EKB) into which said renewal node key is encrypted with a node key or a leaf key in said group, and generating and distributing a message data encrypted by said renewal node key; and

a decrypting processing step of executing decrypting processing on said encrypted message data by using a key set in each device holding said different key set of a node key peculiar to each node in said hierarchical tree structure and a leaf key peculiar to each device.

13. The information processing method according to claim 12 wherein said decrypting processing step includes a renewal node key obtaining step of obtaining said renewal node key by processing of the enabling key block (EKB); and

a message data decrypting step for executing decryption of the encrypted message data by said renewal node key.

14. The information processing method according to claim 12 wherein said message data is a content key capable of being used as a decryption key for decrypting the content data.

15. The information processing method according to claim 12 wherein said message data is an authentication key used in the authentication processing.

16. The information processing method according to claim 12 wherein said message data is a key of generating an integrity check value (ICV) of contents.

17. The information processing method according to claim 12 wherein said

message data is a program code.

18. The information processing method according to claim 12 wherein said message data distributing means distributes said enabling key block (EKB) and an encrypted data comprising a content key usable as a decryption key for decrypting content data as said message data and an encrypted content encrypted by said content key.

19. The information processing method according to claim 12 wherein said message data distributing means and said device respectively have an authentication processing means for executing authentication processing, and

wherein a distribution of said message data is performed on the condition that authentication processing between said message data distributing means and said device has been completed.

20. The information processing method according to claim 12 wherein there exists a different intermediate device between said message data distributing means and said device, and

wherein said message data distributing means generates and distributes an enabling key block (EKB) and an encrypted message data that can be decrypted only in a target device targeted for distributing said message data.

21. An information recording medium having stored therein data, storing:

a renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected at subordinate of the top node which is

one node of the hierarchical tree structure having a plurality of different devices as leaves is renewed and an enabling key block (EKB) into which said renewal node key is encrypted by a node key or a leaf key in said group; and

a message data encrypted by said renewal node key.

22. The information recording medium according to claim 21 wherein said message data is a content key used for decrypting contents, and

wherein said information recording medium stores an encrypted content encrypted by said renewal node key.

23. The information recording medium according to claim 22 wherein said information recording medium stores correspondence data for relating a content with an enabling key block (EKB) used for obtaining a content key corresponding to said content.

24. The information recording medium according to claim 21 wherein said information recording medium stores an integrity check value (ICV) of contents.

25. A program providing medium for providing a computer program for executing decrypting process of encrypted content data on a computer system, said computer program comprising:

a renewal node key obtaining step of obtaining a renewal node key by decrypting process of an enabling key block (EKB) into which said renewal node key into which at least one of the node keys in a group constituted by nodes and a leaf connected at subordinate of the top node which is one node of the hierarchical

tree structure having a plurality of different devices as leaves is renewed is encrypted with a node key or a leaf key in a group on a renewal node key;

a step of executing decrypting process by said renewal node key to obtain a content key used as a decryption key for said encrypted content; and

a step of executing decryption of said encrypted content by said content key.

26. An information processing method for distributing encrypted message data capable of being used only in not less than one device selected, comprising the steps of:

generating a renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected at subordinate of a top node which is one node of the hierarchical tree structure having a plurality of different devices as leaves is renewed, and an enabling key block (EKB) into which said renewal node key is encrypted by a node key or a leaf key in said group; and

generating a message data encrypted with said renewal node key to distribute it to devices.

27. The information processing method according to claim 26 wherein said message data is a content key capable of being used as a decryption key for decrypting the content data.

28. The information processing method according to claim 26 wherein said message data is an authentication key used in the authentication processing.

29. The information processing method according to claim 26 wherein said

Art 19 Amendment

message data is a key of generating an integrity check value (ICV) of contents.

30. The information processing method according to claim 26 wherein said enabling key block (EKB) and an encrypted data is distributed, said encrypted data comprising a content key usable as a decryption key for decrypting content data as said message data and an encrypted content encrypted with said content key.

31. An information processing method comprising:

a renewal node key obtaining step of obtaining a renewal node key by decrypting processing of an enabling key block (EKB) into which said renewal node key into which at least one of the node keys in a group constituted by nodes and a leaf connected to a subordinate of a top node which is one node of a hierarchical tree structure having a plurality of different devices as leaves is renewed is encrypted with a node key or a leaf key in said group ;

a content key obtaining step of executing decryption process with said renewal node key to obtain a content key used as a decryption key for said encrypted content; and

an executing step of executing decrypting of said encrypted content by said content key.

10/009076
JC10 Rec'd PCT/PTO 0 3 DEC 2001

32. (Added) An information processing system for distributing encrypted message data capable of being used only in not less than one device selected,

said individual device comprising:

encryption processing means for holding a different key set of a node key peculiar to each node in a hierarchical tree structure with a plurality of different devices as leaves and a leaf key peculiar to each device and executing decrypting process on said encrypted message data distributed to a device using said key set;

wherein a message data distributing means generates a renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected at subordinate of a top node which is one node of the hierarchical tree structure is renewed and an enabling key block (EKB) into which said renewal node key is encrypted with a node key or a leaf key in said group, and generating and distributing a message data encrypted with said renewal node key,

wherein said message data distributing means generates an encrypted message data encrypted by using said renewal node key and an enabling key block (EKB) containing one or more renewal node keys encrypted by using a leaf key or a node key that is not held by devices other than said selected device, and distributes said encrypted message data and said enabling key block,

wherein said selected device decrypts said encrypted message data with said key set held by said selected device only and said enabling key block into an original message data.

Art. 19 Amendment

33. (Added) An information processing apparatus comprising:

key set storing means for holding one of the different key sets of a node key peculiar to each node in a hierarchical tree structure with a plurality of different devices as leaves and a leaf key peculiar to each device, each of said key sets being prescribed differently; and

encrypted processing means for decrypting an encrypted data by using said node key and said leaf key stored in said key set storing means or a key distributed,

wherein said encrypted processing means wherein decryption of a encrypted message data with a renewal node key by decrypting a renewal node key with which said message data is encrypted with a leaf key or a node key held in said key set storing means is made on encrypted data containing a message data encrypted with a renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected at subordinate of a top node which is one node of the hierarchical tree structure is renewed and an enabling key block (EKB) containing one or more renewal node keys encrypted by using a leaf key or a node key that is not held by devices other than said selected device.